



Fair Exchange with Guardian Angels

Gildas AVOINE & Serge VAUDENAY

<http://lasecwww.epfl.ch>

Swiss Federal Institute of Technology (EPFL)

This work is supported by the National Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS), a center supported by the Swiss National Science Foundation.



Outline

- Some recalls on Fair Exchange
- Synchronization Problem
- Pirates and Guardian Angels
- Analysis of the protocol



- ▶ **Some recalls on Fair Exchange**
 - Synchronization Problem
 - Pirates and Guardian Angels
 - Analysis of the protocol

Some recalls on Fair Exchange



Fair Exchange: Definition

An exchange protocol is said to be **fair** if it ensures that during the exchange of the items, no party involved in the protocol can gain an advantage over the other party, even if the protocol is halted for any reason.



Perfect Fair Exchange

A fair exchange protocol is said to be **perfect** if it is **complete** and **timely**.



Perfect Fair Exchange

A fair exchange protocol is said to be **perfect** if it is **complete** and **timely**.

Complete: Both participants always receive the expected items if they are honest.



Perfect Fair Exchange

A fair exchange protocol is said to be **perfect** if it is **complete** and **timely**.

Complete: Both participants always receive the expected items if they are honest.

Timely: The exchange eventually ends.



The simplest exchange protocol



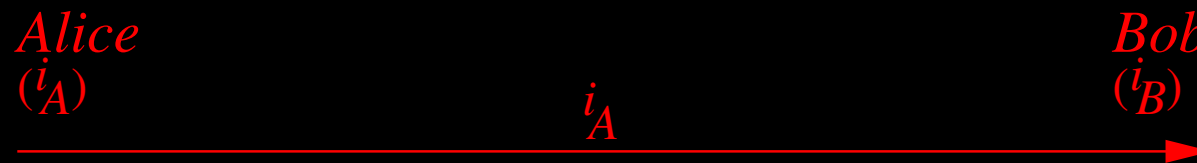
The simplest exchange protocol

Alice
 (i_A)

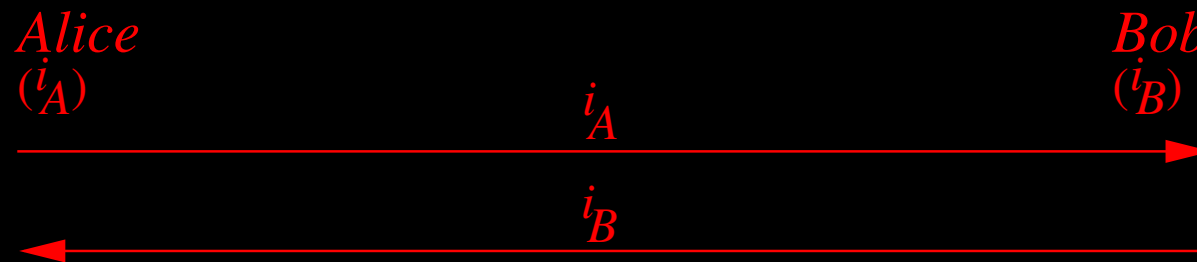
Bob
 (i_B)



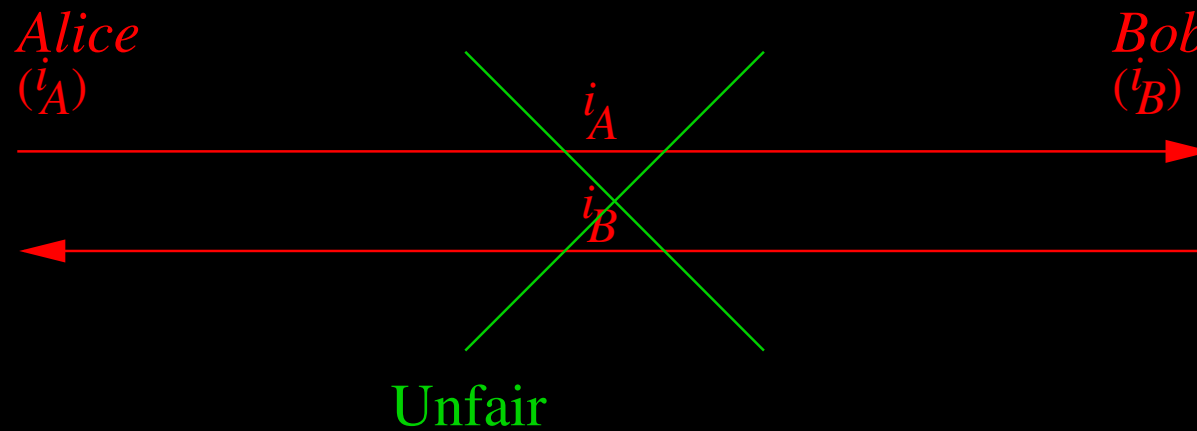
The simplest exchange protocol



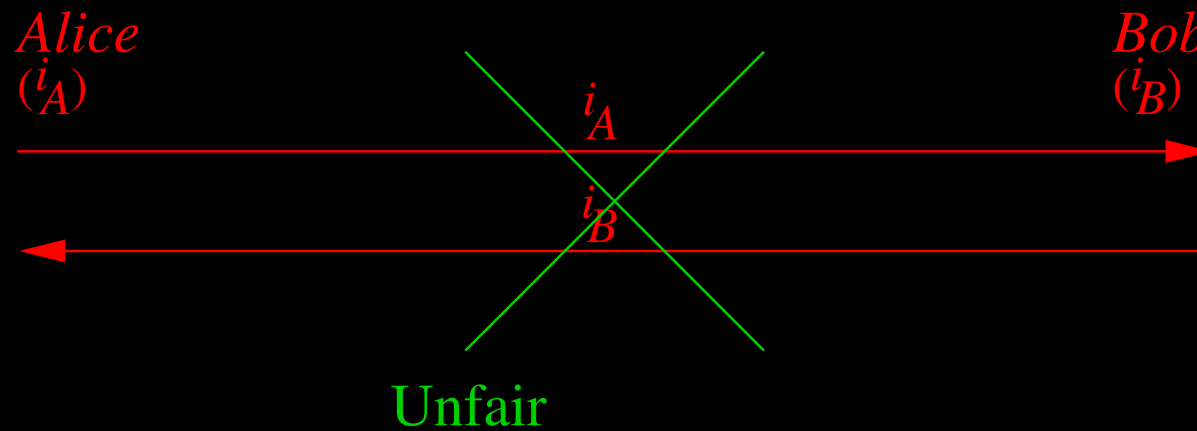
The simplest exchange protocol



The simplest exchange protocol



The simplest exchange protocol



[Even and Yacobi, 1980]

Fair Exchange: Classification

- Perfect (Using a Trusted Third Party)
 - On-line
 - Off-line
- Unperfect
 - Gradual
 - Probabilistic



FE with an on-line TTP



FE with an on-line TTP

A

TTP

B



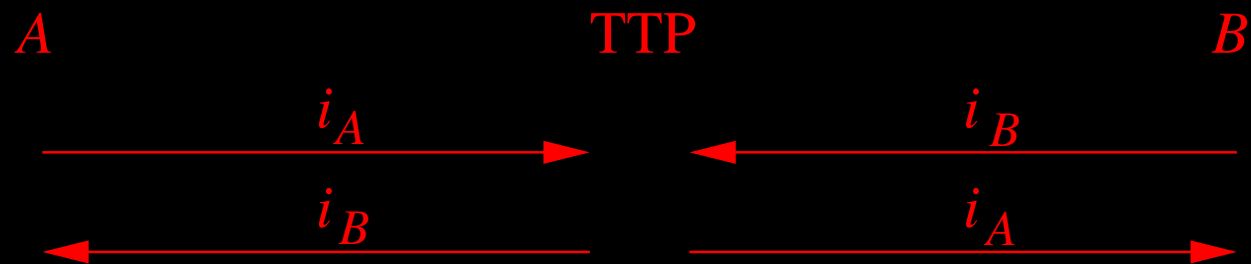
FE with an on-line TTP



FE with an on-line TTP



FE with an on-line TTP



FE with an on-line TTP

Advantage:

- Can be used to exchange arbitrary types of items.

Drawbacks:

- Having an online Third Party is a strong requirement.
- The Third Party needs to be trusted.
- The Third Party becomes a bottleneck.



FE with an off-line TTP



FE with an off-line TTP

→ Main protocol (without TTP).



FE with an off-line TTP

- Main protocol (without TTP).
- Recovery protocol (with TTP).



FE with an off-line TTP

- Main protocol (without TTP).
- Recovery protocol (with TTP).
- Abort protocol.



FE with an off-line TTP



FE with an off-line TTP

A

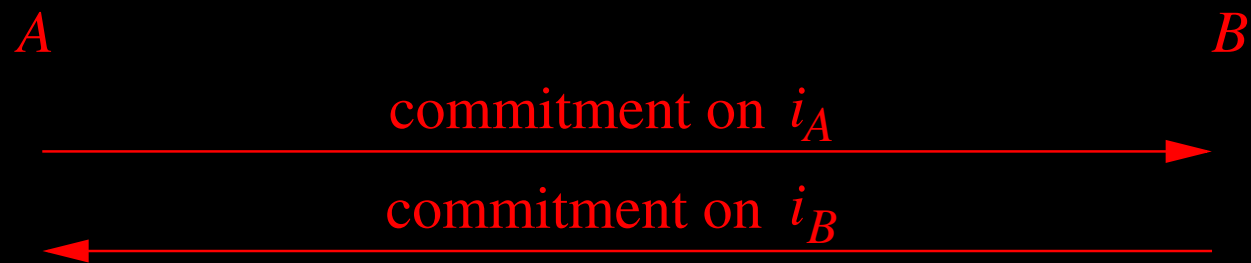
B



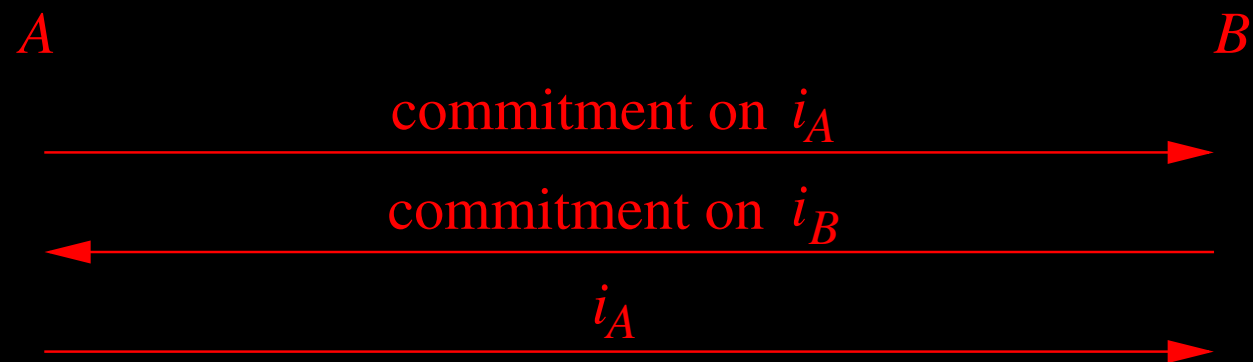
FE with an off-line TTP



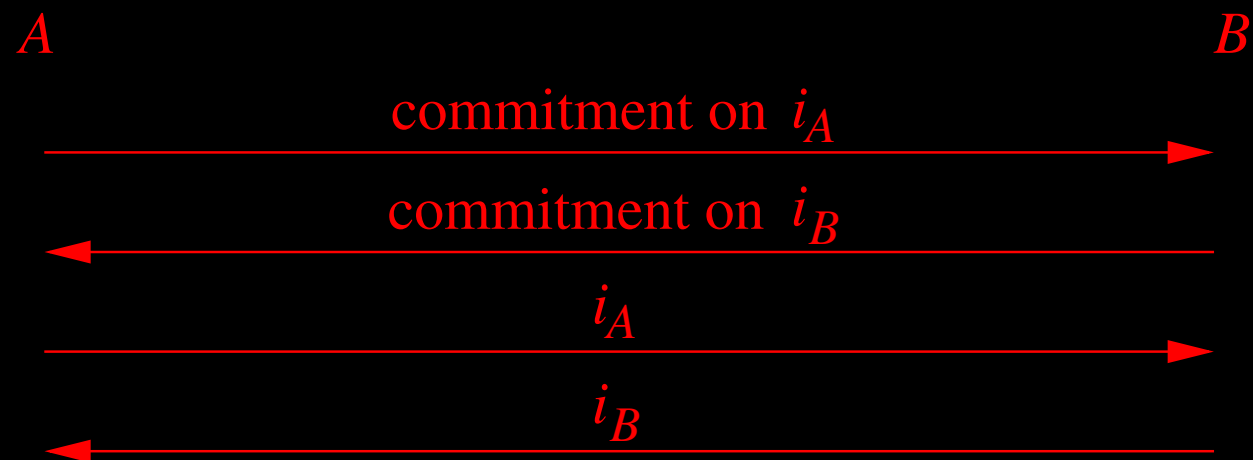
FE with an off-line TTP



FE with an off-line TTP



FE with an off-line TTP



FE with an off-line TTP

Advantage:

- The TTP is required only in case of conflict.

Drawbacks:

- Having a Third Party is sometimes difficult to achieve (even off-line)
- The Third Party needs to be trusted.
- The items must be revocable or generatable.



Gradual FE

Each entity alternatively transmits successive pieces of the items to exchange until the last piece of each item was sent.



Gradual FE

Each entity alternatively transmits successive pieces of the items to exchange until the last piece of each item was sent.

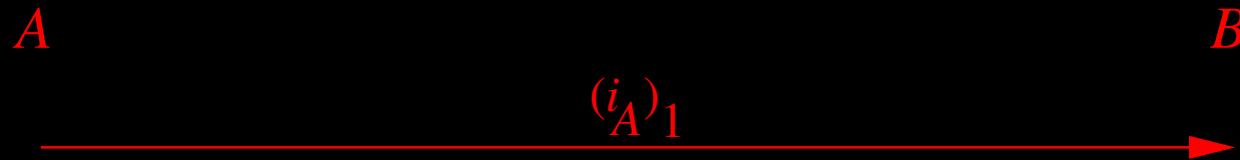
A

B



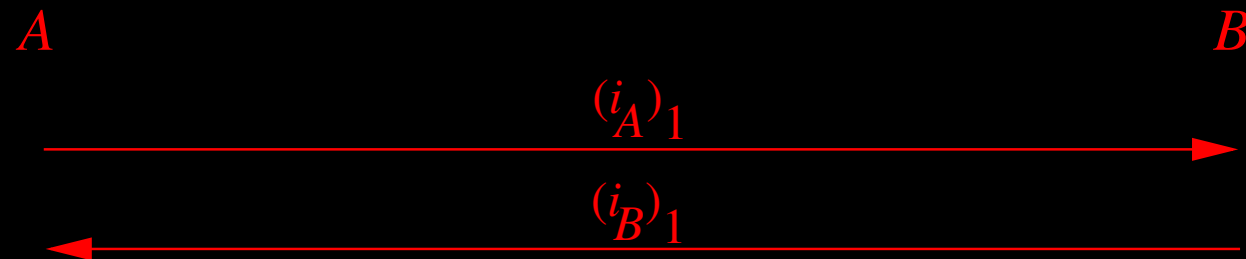
Gradual FE

Each entity alternatively transmits successive pieces of the items to exchange until the last piece of each item was sent.



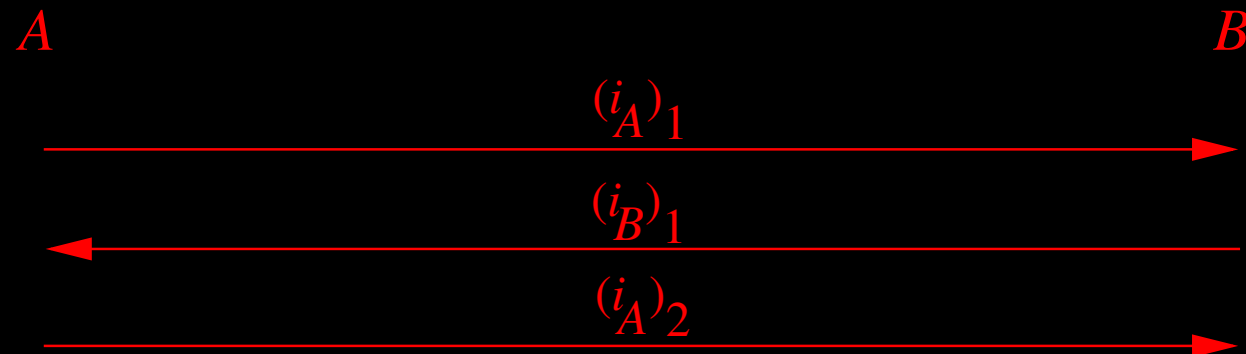
Gradual FE

Each entity alternatively transmits successive pieces of the items to exchange until the last piece of each item was sent.



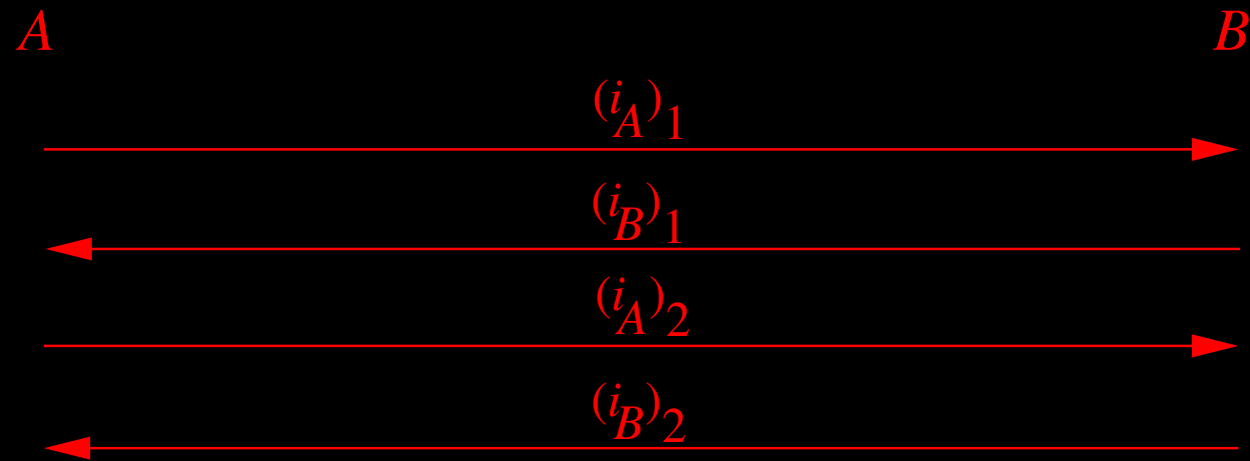
Gradual FE

Each entity alternatively transmits successive pieces of the items to exchange until the last piece of each item was sent.



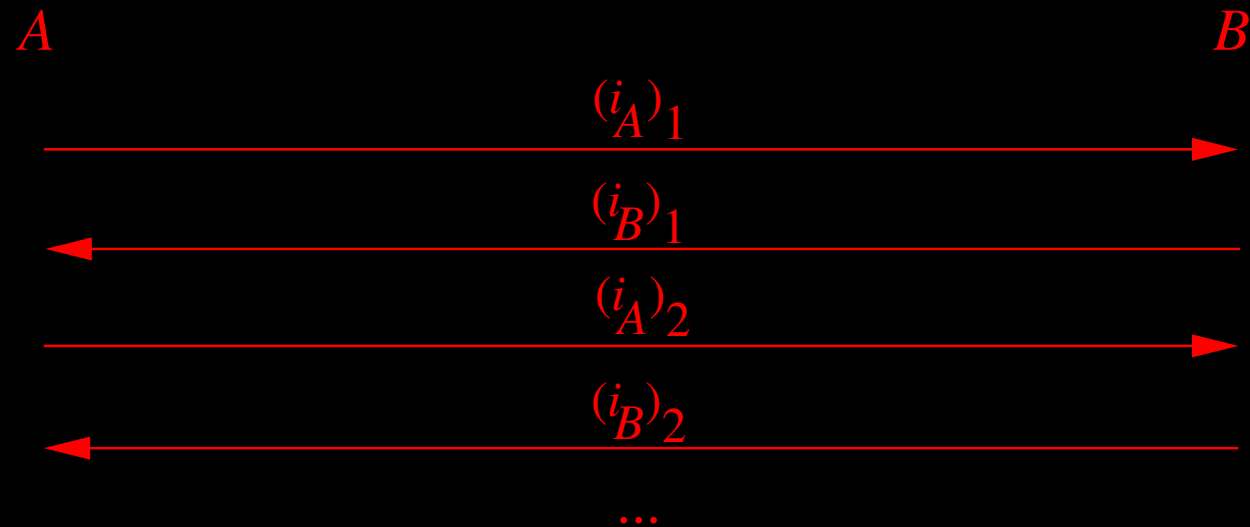
Gradual FE

Each entity alternatively transmits successive pieces of the items to exchange until the last piece of each item was sent.



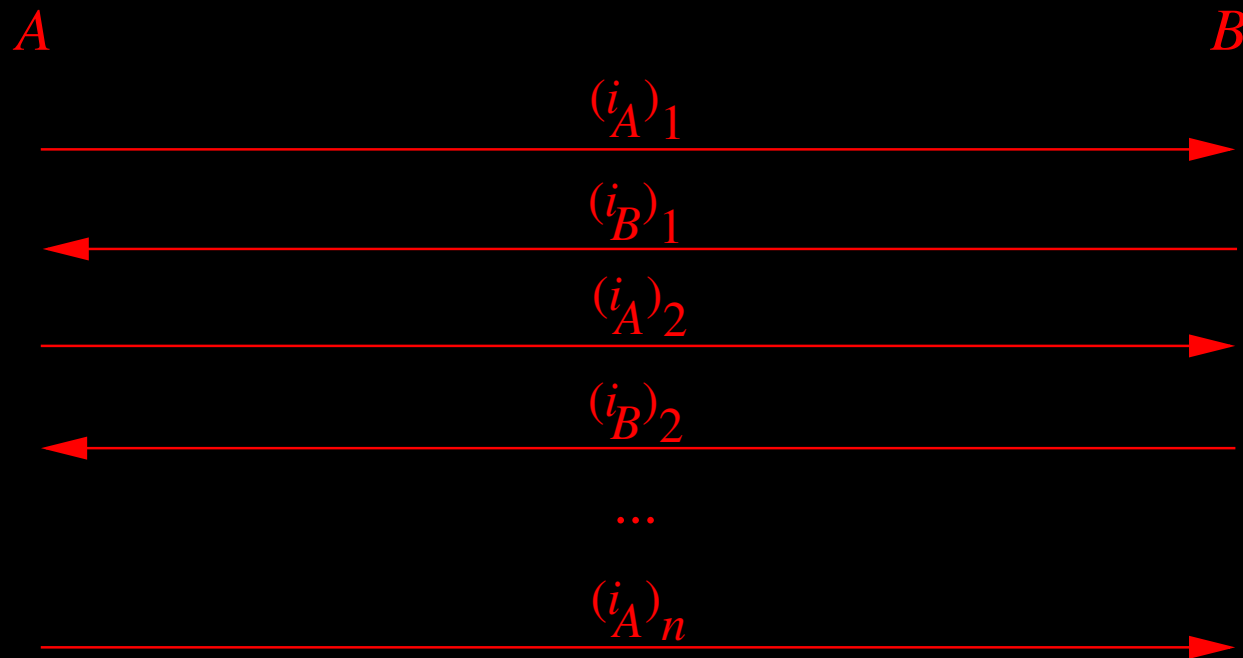
Gradual FE

Each entity alternatively transmits successive pieces of the items to exchange until the last piece of each item was sent.



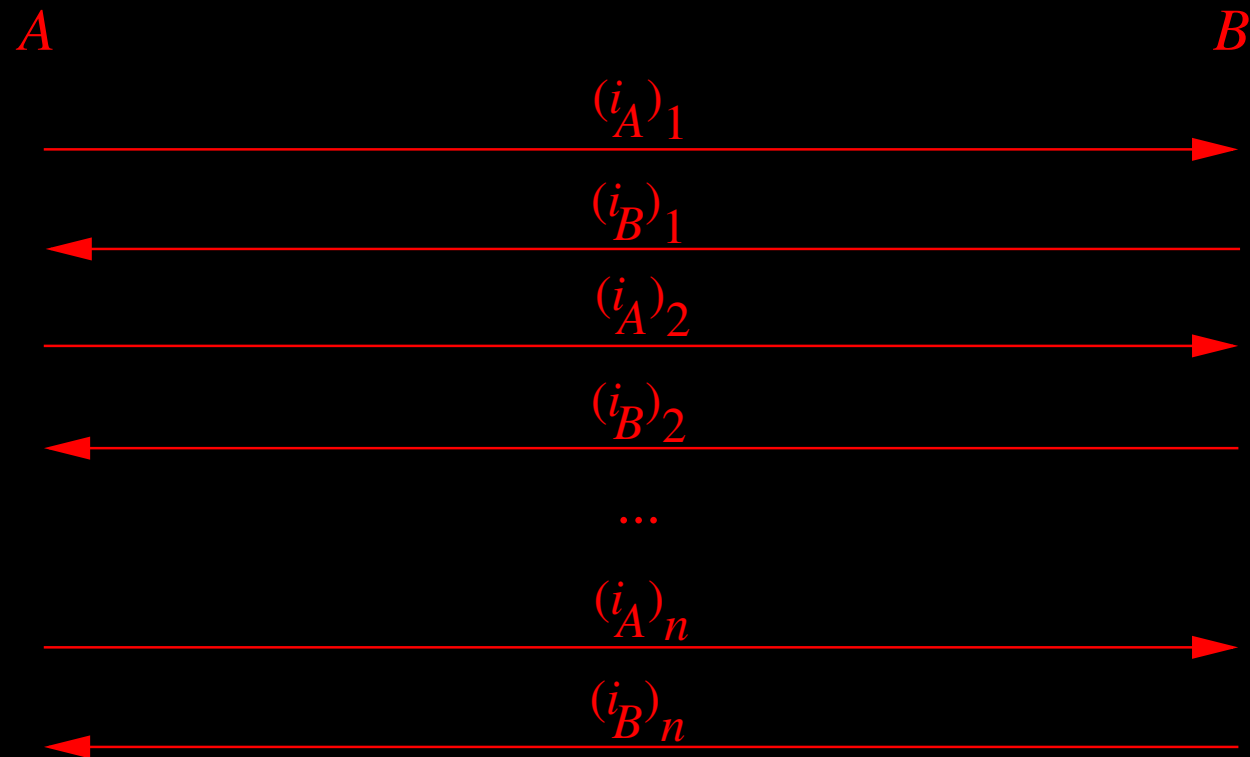
Gradual FE

Each entity alternatively transmits successive pieces of the items to exchange until the last piece of each item was sent.



Gradual FE

Each entity alternatively transmits successive pieces of the items to exchange until the last piece of each item was sent.



Gradual FE

Advantage:

- This model does not require a TTP.

Drawbacks:

- High communication overhead.
- Difficult to determine if $(i_X)_j$ is really a part of i_X .
- The two participants must have the same computational power.
- Fairness is not ensured during the protocol.



Probabilistic FE

Our goal is to design a **probabilistic** Fair Exchange protocol.

To achieve this task, we are going to reduce the Fair Exchange Problem to the Synchronization Problem.



Some recalls on Fair Exchange

▶ **Synchronization Problem**

Pirates and Guardian Angels

Analysis of the protocol

Synchronization Problem



Synchronization: Definition

A synchronization protocol between A and B is a protocol which eventually ends with A and B on two possible terminal states, either **success** or **failure**.

Complete: A and B always end on the success state when there is no malicious misbehavior.

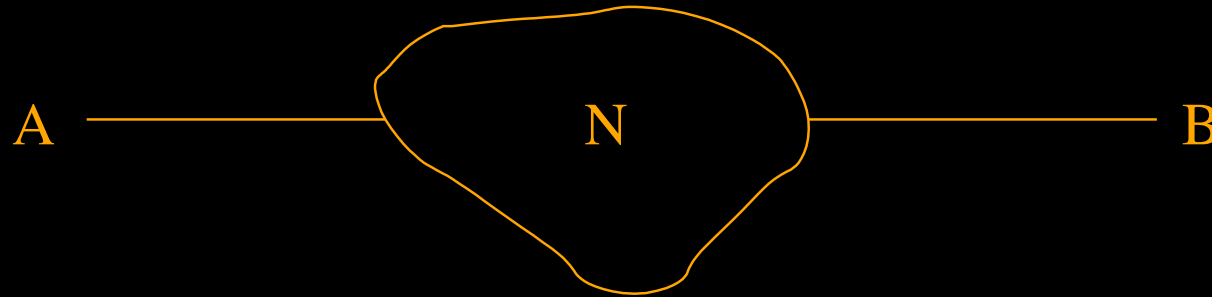
Fair: A and B always end on the same state even in case of misbehavior.

Timely: A and B eventually end.



Synchronization Problem

How can two **honest** participants A and B achieve a synchronization through a malicious network N which may want to harm A or B ?



A and B are able to establish a secure channel providing confidentiality, authenticity, integrity, and sequentiality.



Synchronization

A

B



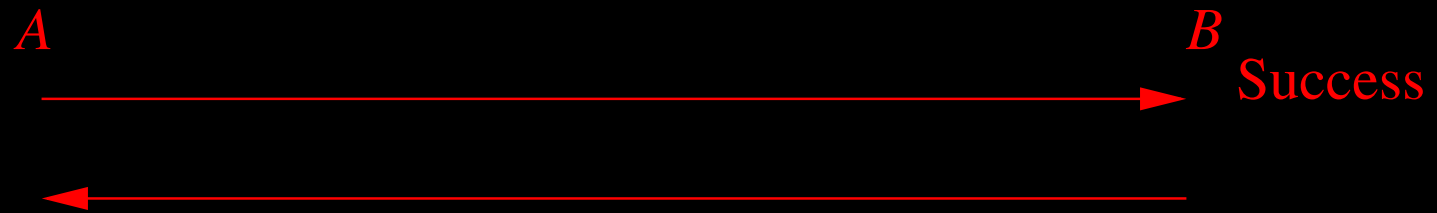
Synchronization



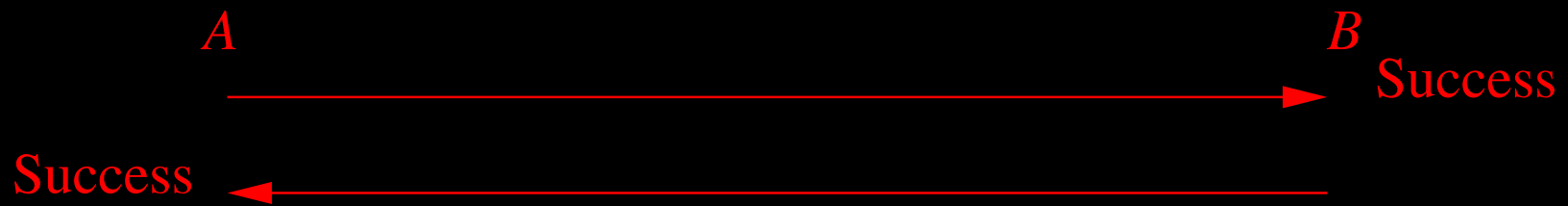
Synchronization



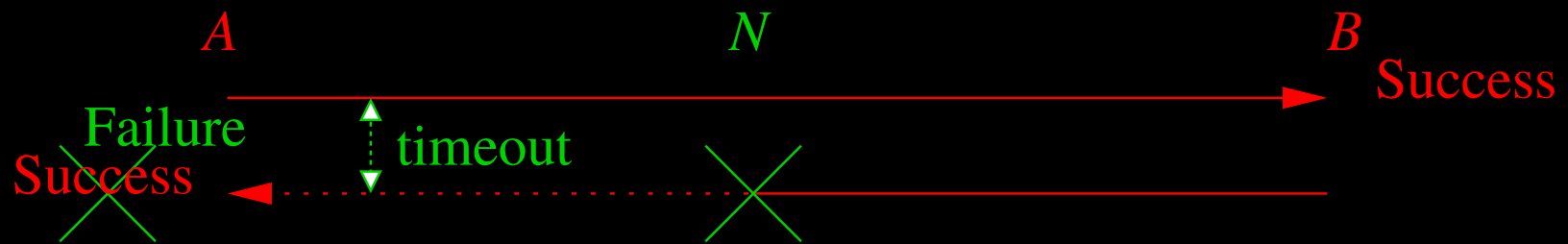
Synchronization



Synchronization



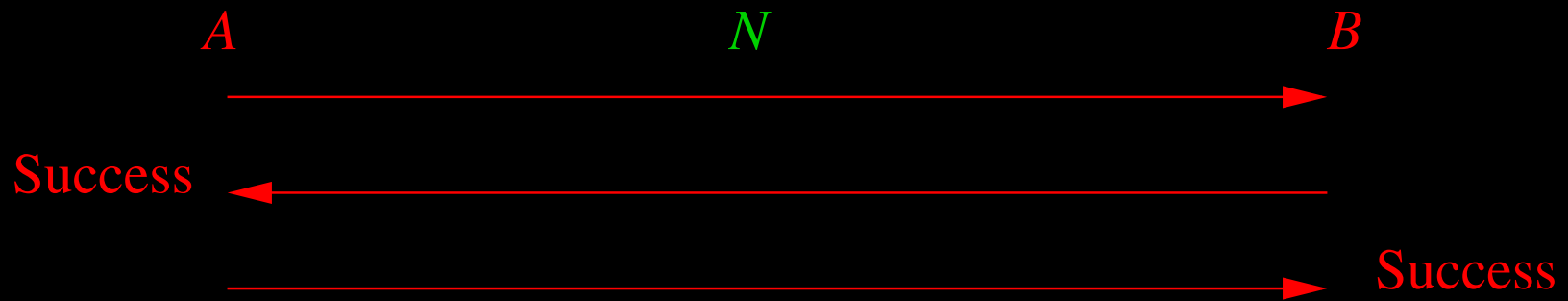
Synchronization



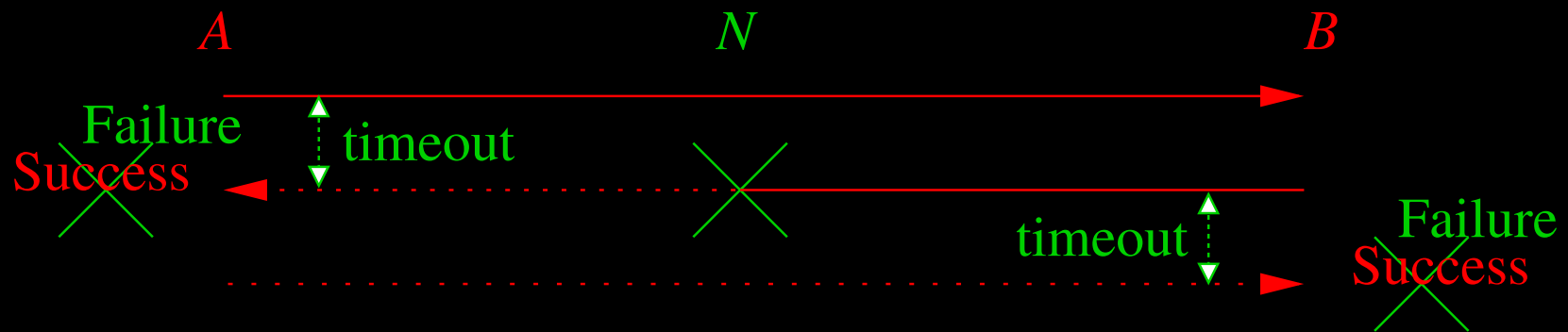
Synchronization



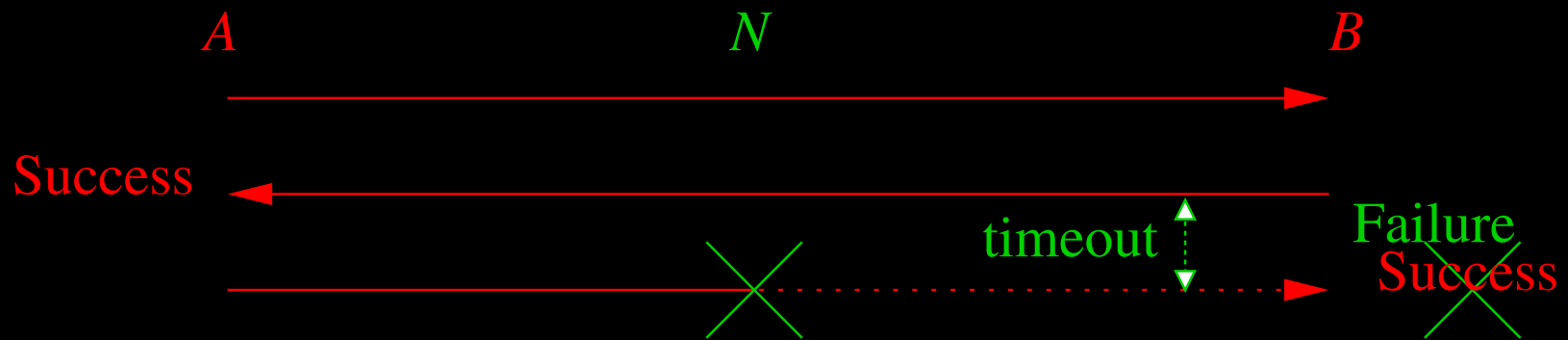
Synchronization



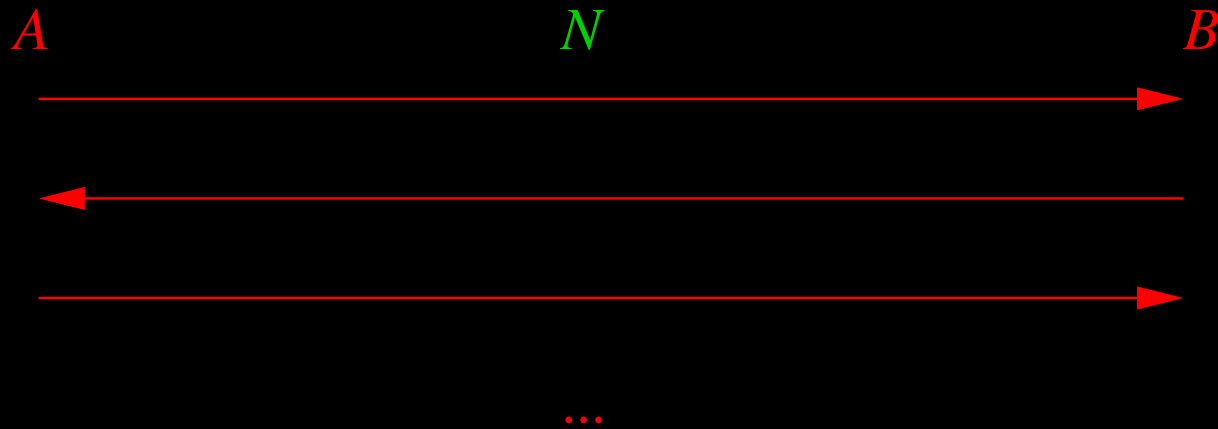
Synchronization



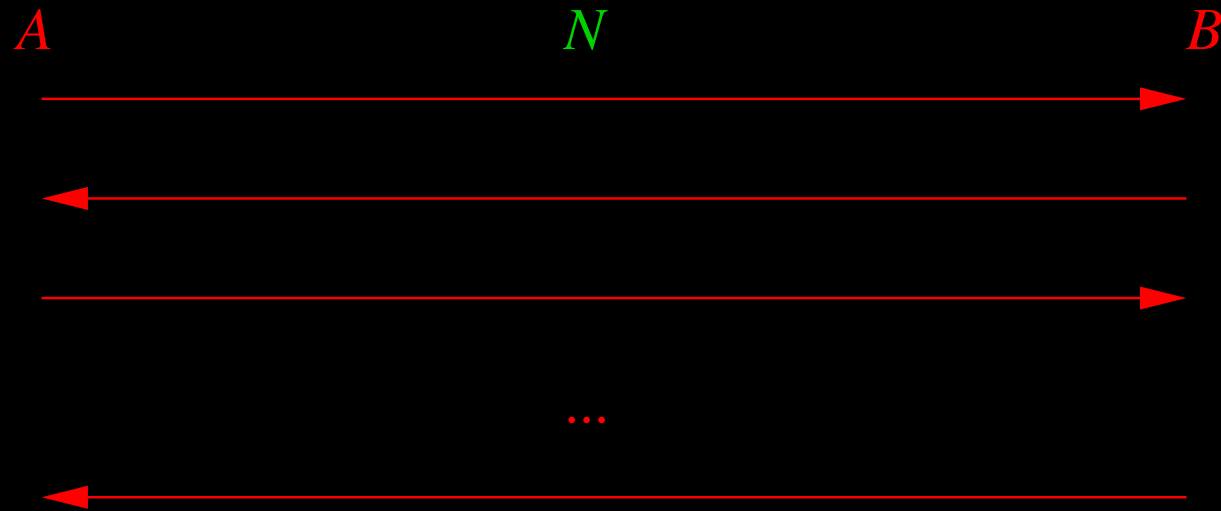
Synchronization



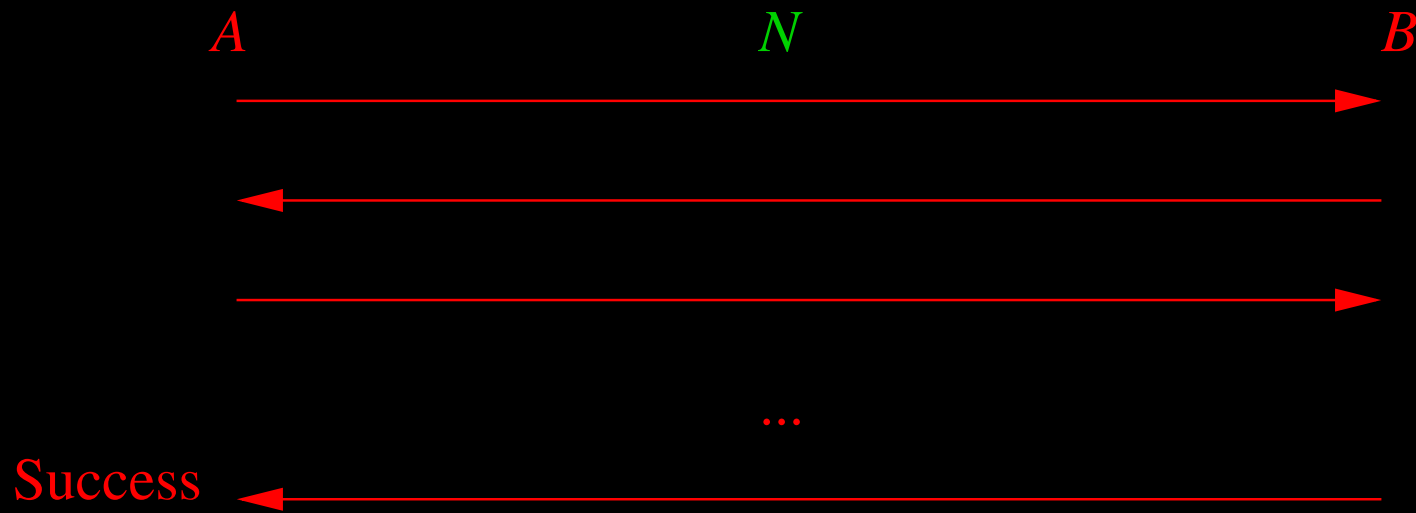
Synchronization



Synchronization



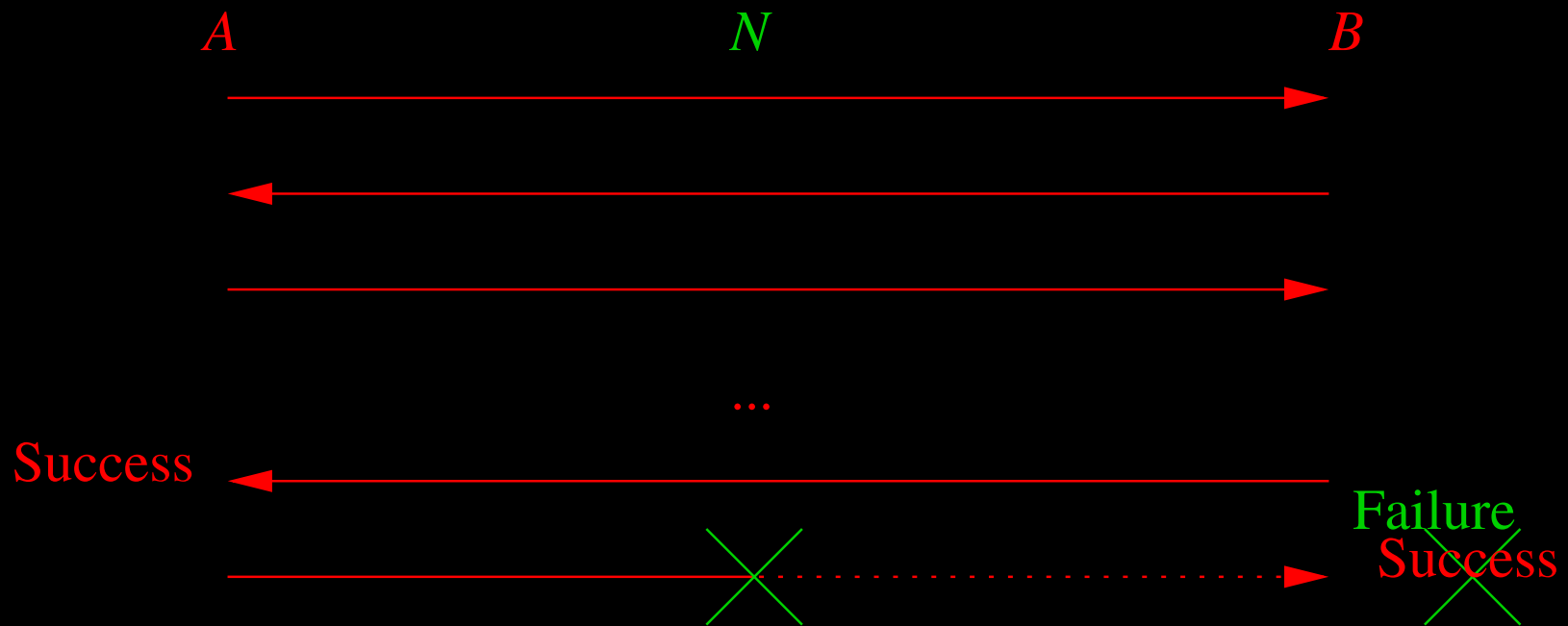
Synchronization



Synchronization



Synchronization

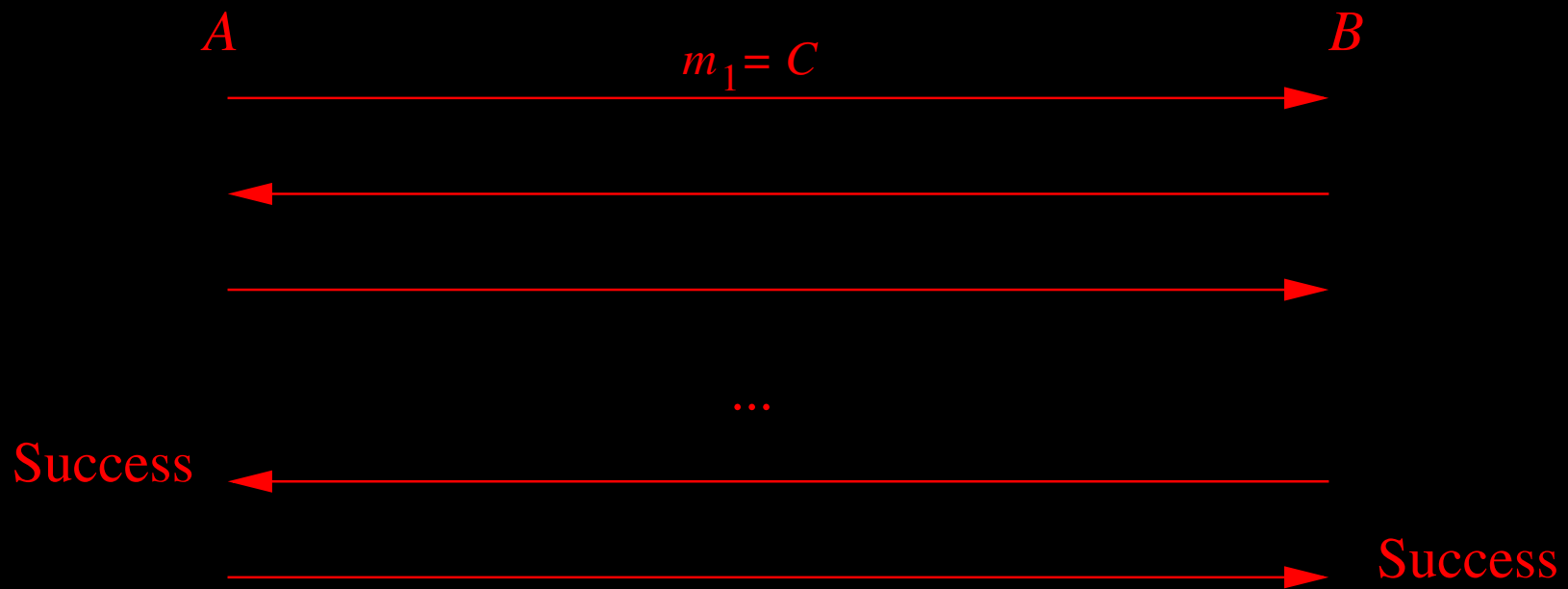


Synchronization

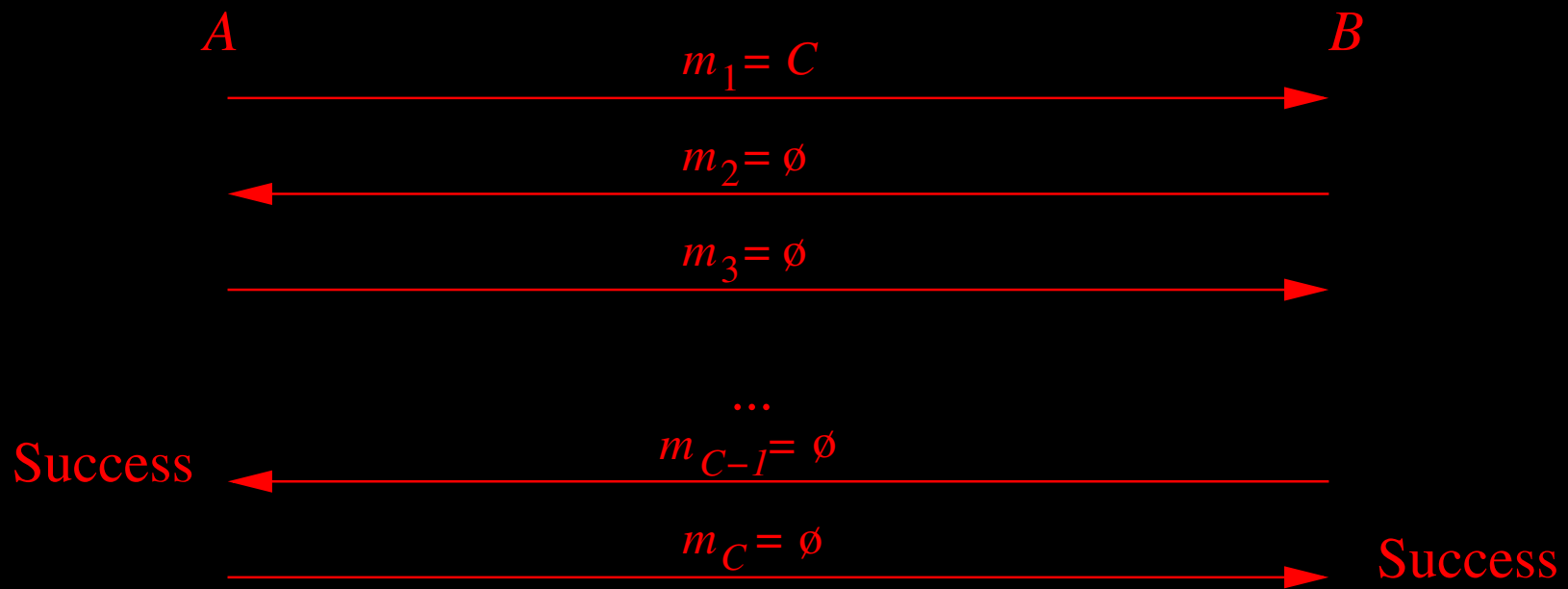
N should not know the number of expected messages (denoted by C) in order to achieve a synchronization protocol in a probabilistic way!



Our Synchronization Protocol



Our Synchronization Protocol



Synchronization

Here A and B was honest: this frame is not the common one for the fair exchange problem!

We design now a model with potential misbehaviors.



Some recalls on Fair Exchange
Synchronization Problem

- ▶ **Pirates and Guardian Angels**
Analysis of the protocol

From Observers...

...to Pirates and Guardian Angels



From Observers...

Introduced by Chaum and Pedersen (1992).

An **Observer** is a security module connected to a device.

- Observers are tamper-proof.
- Observers are simple and limited.
- Observers have a single i/o port (connected to their own device)



...to Pirates and Guardian Angels

A **Guardian Angel** is a honest Observer, connected to a potentially misbehaving device, a **Pirate**.

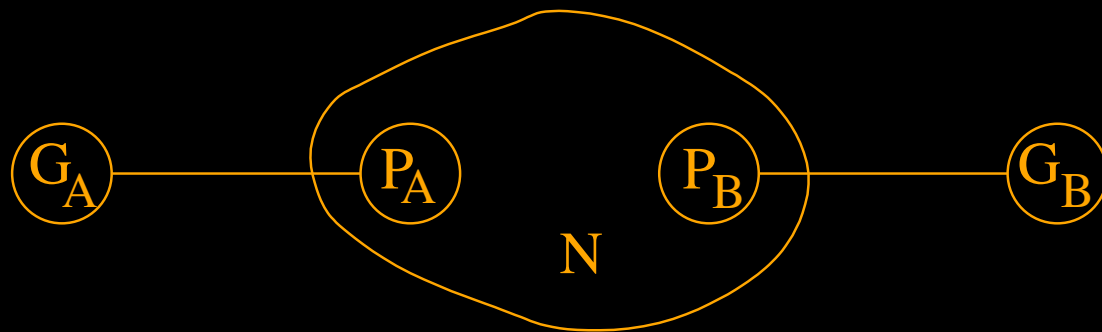
A **Pirate** is powerful in the sense that he is able to communicate with all the other Pirates and his own Guardian Angel. We require no assumption on his computational capabilities.



...to Pirates and Guardian Angels

A **Guardian Angel** is a honest Observer, connected to a potentially misbehaving device, a **Pirate**.

A **Pirate** is powerful in the sense that he is able to communicate with all the other Pirates and his own Guardian Angel. We require no assumption on his computational capabilities.



Our FE Protocol



Our FE Protocol

G_A

P_A

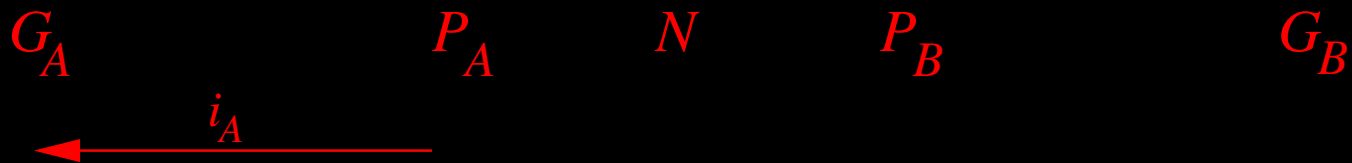
N

P_B

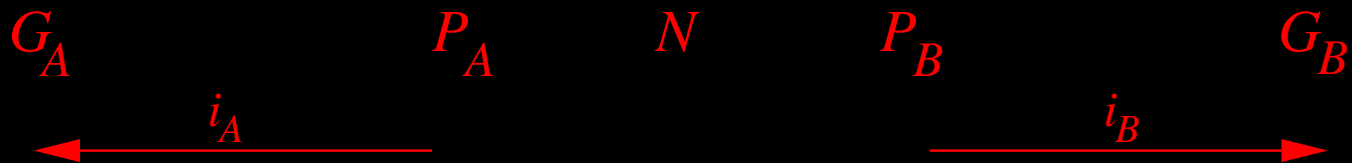
G_B



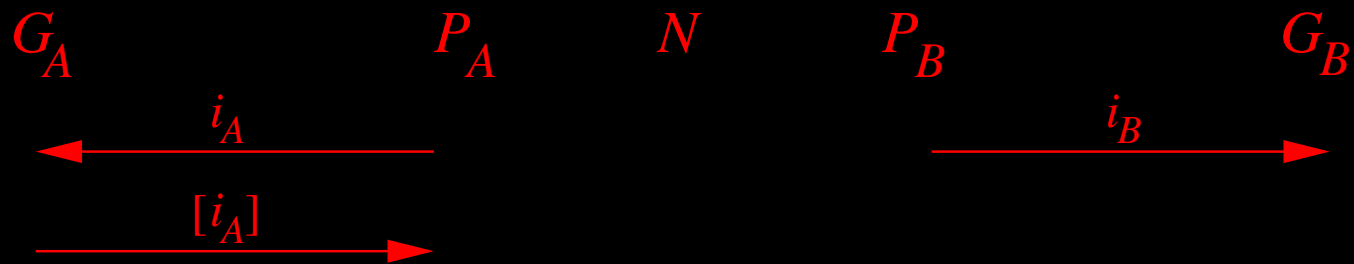
Our FE Protocol



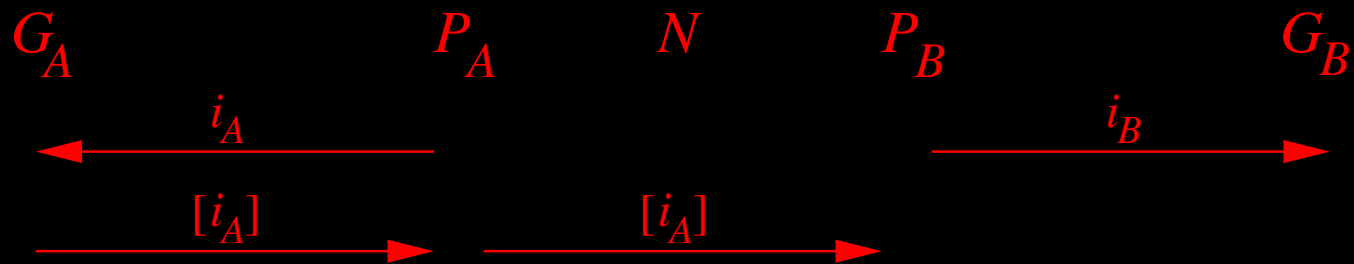
Our FE Protocol



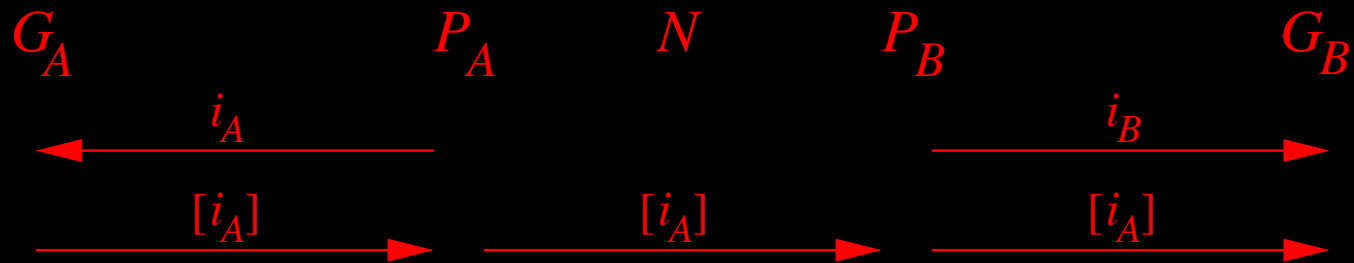
Our FE Protocol



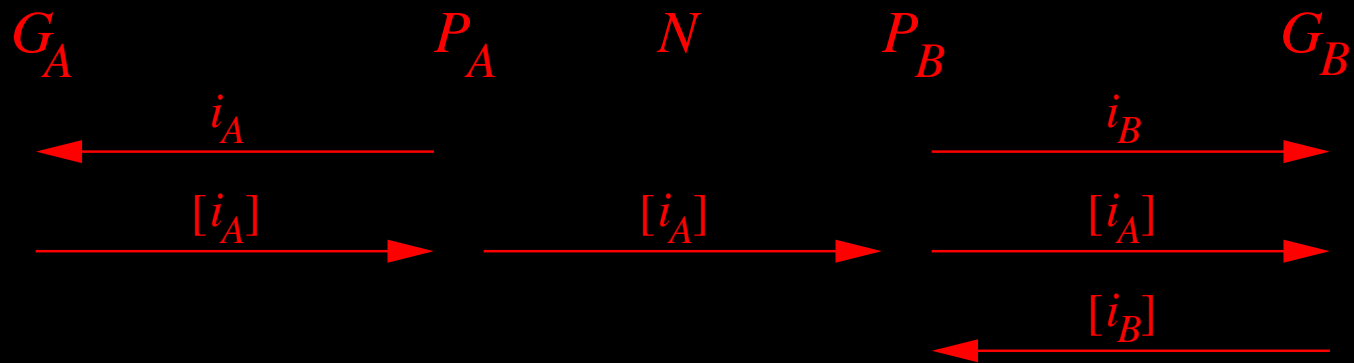
Our FE Protocol



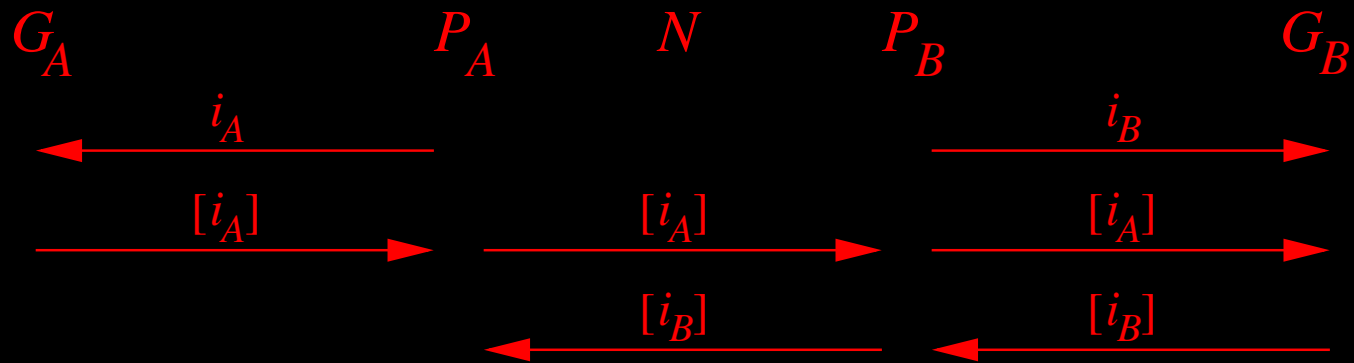
Our FE Protocol



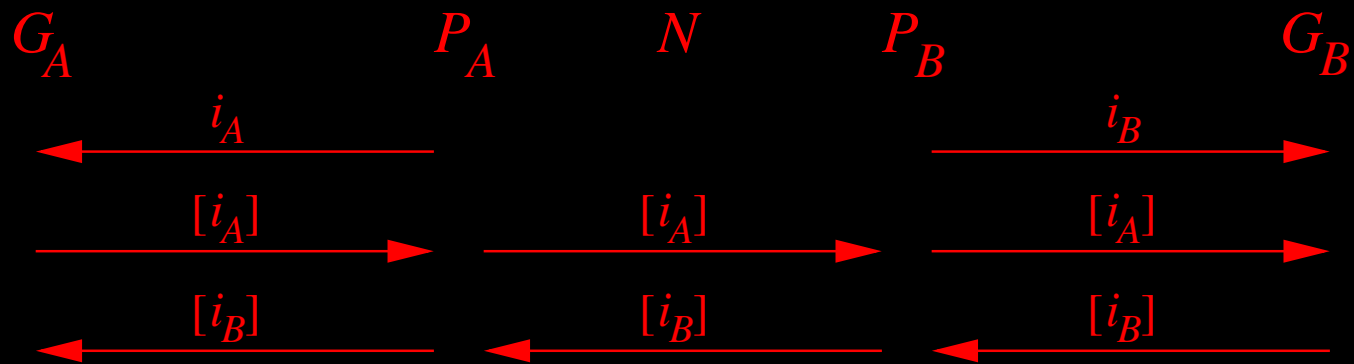
Our FE Protocol



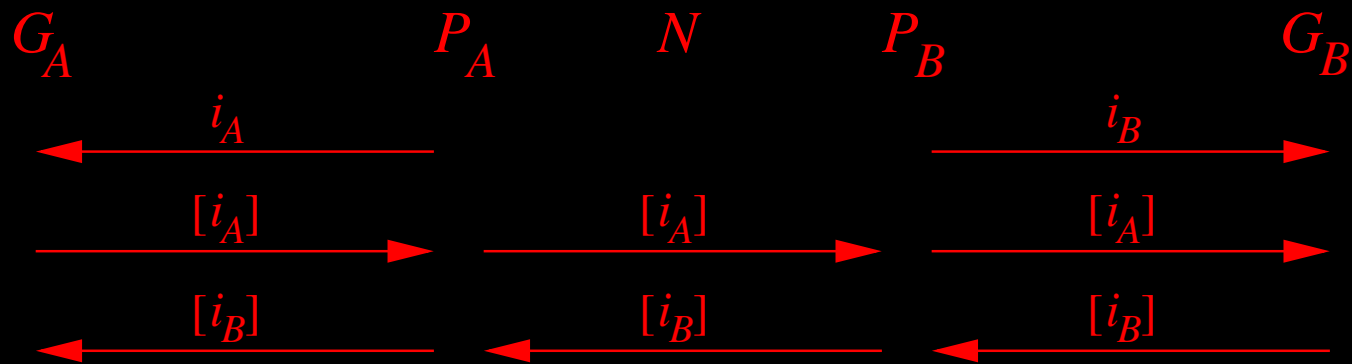
Our FE Protocol



Our FE Protocol

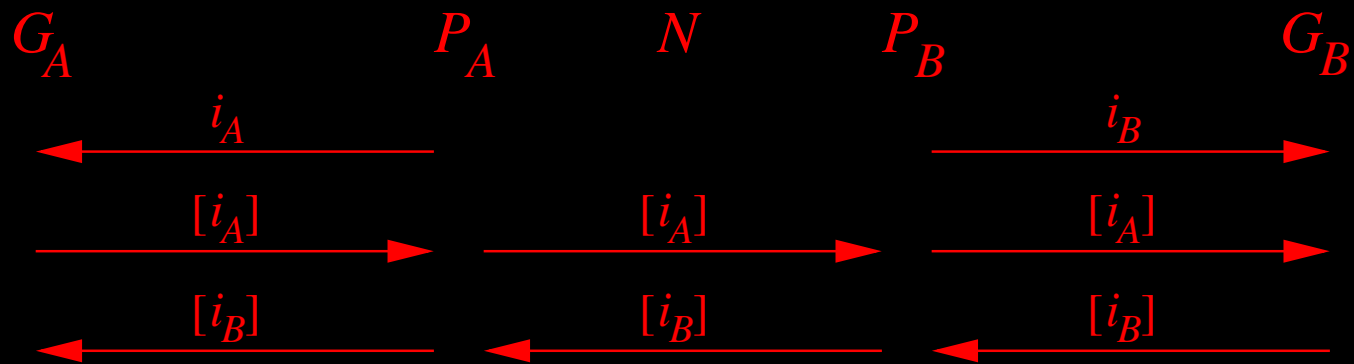


Our FE Protocol



Synchronization Protocol

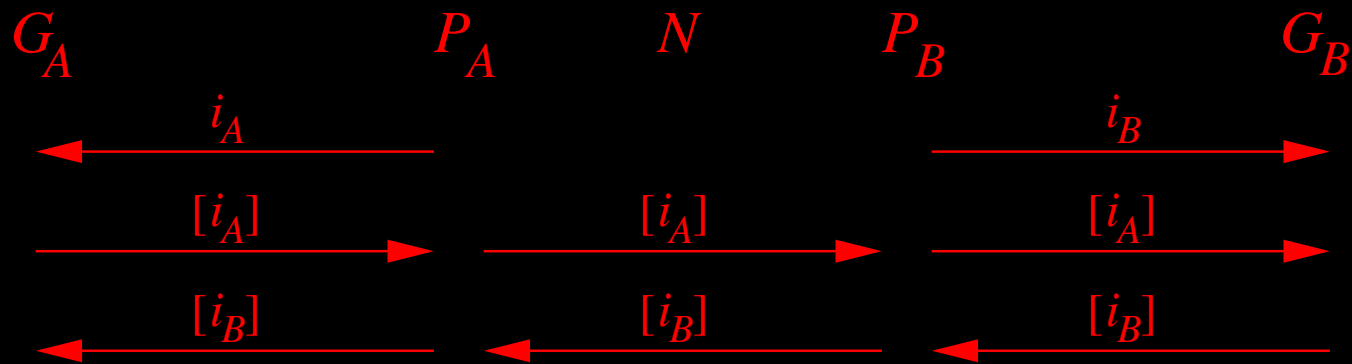
Our FE Protocol



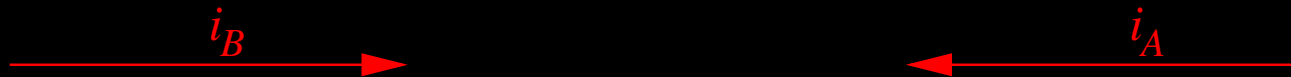
Synchronization Protocol



Our FE Protocol



Synchronization Protocol



Some recalls on Fair Exchange
Synchronization Problem
Pirates and Guardian Angels
▶ Analysis of the protocol

Analysis of the protocol



Complexity

When P_A and P_B are honest, the complexity in terms of exchanged messages is exactly equal to C .

When something misbehaves, the complexity is smaller.

Let p_i be the probability $\Pr[C = i]$; by definition, the average complexity is

$$E(C) = \sum_{i=1}^{+\infty} ip_i.$$



Probabilities

P_a (**probability of unfairness**) is the maximum of the probability that the protocol ends on an unfair state (over all possible misbehavior of N).

P_c (**probability that crime pays**) is the maximum of the conditional probability that the protocol ends on an unfair state conditioned on N deviating from the protocol (over all possible misbehavior of N).



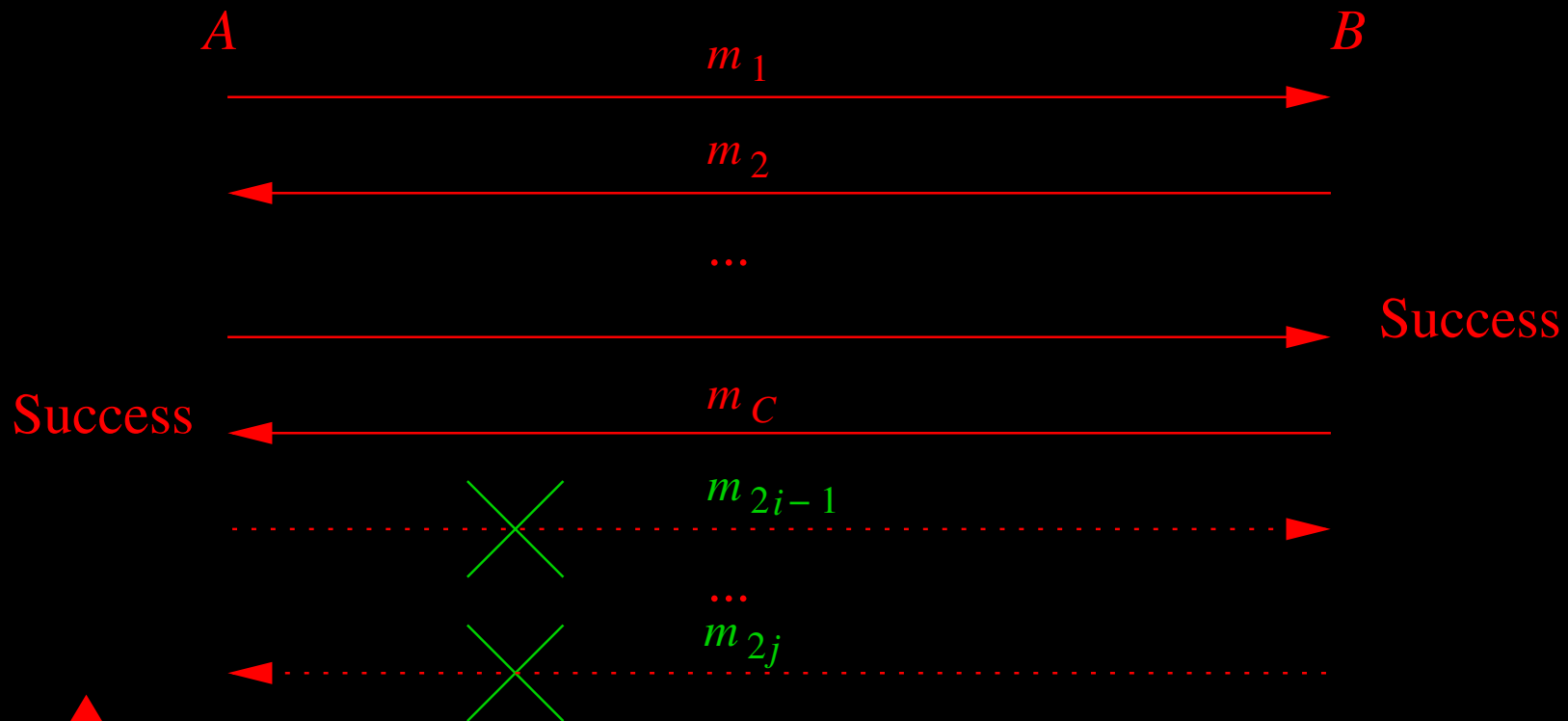
Probability of unfairness (1)

Assume that P_A is willing to drop the $(2i - 1)$ th message and that P_B is willing to drop the $2j$ th one.



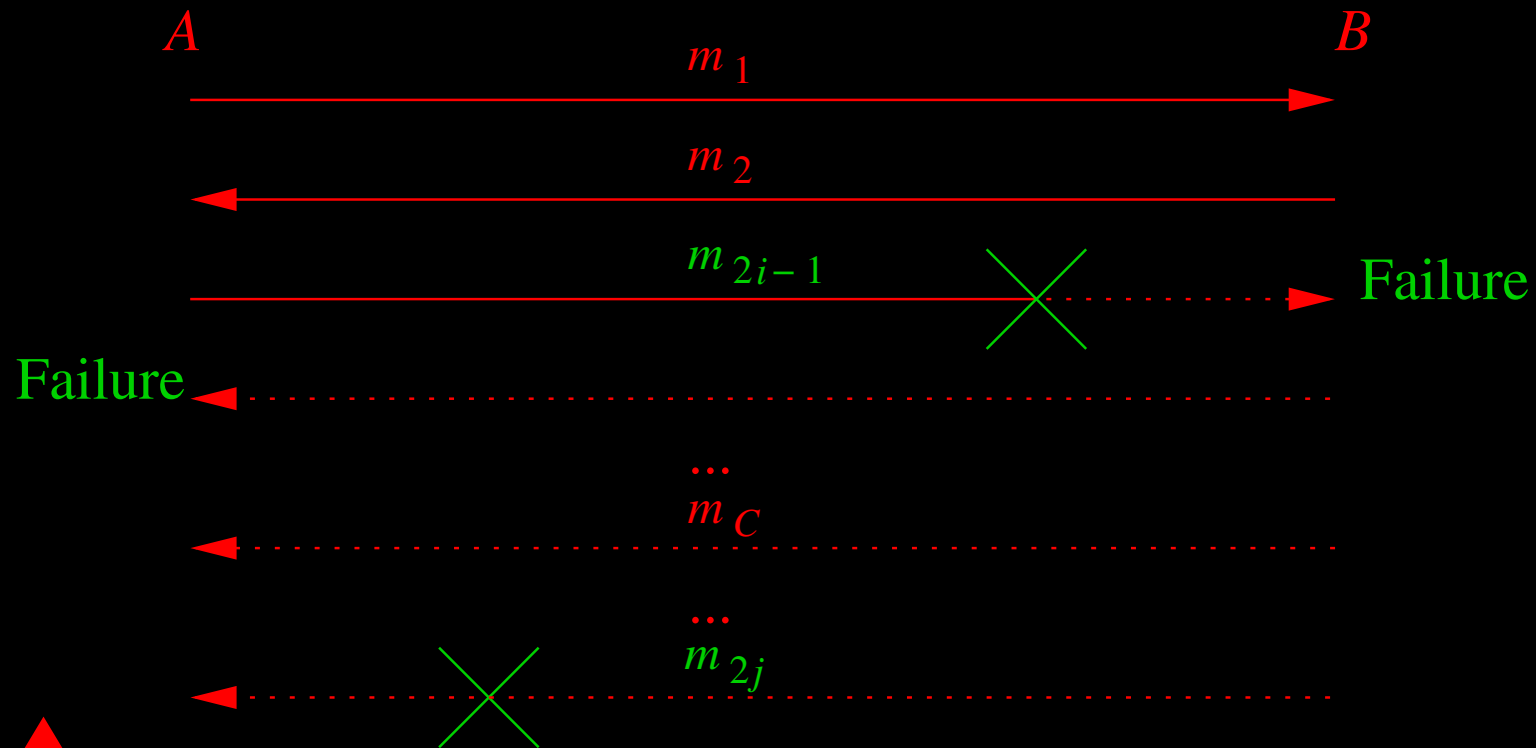
Probability of unfairness (2)

If $C < 2i - 1$ and $C < 2j$ then the misbehavior of P_A and P_B have no influence and the protocol fairly succeeds.



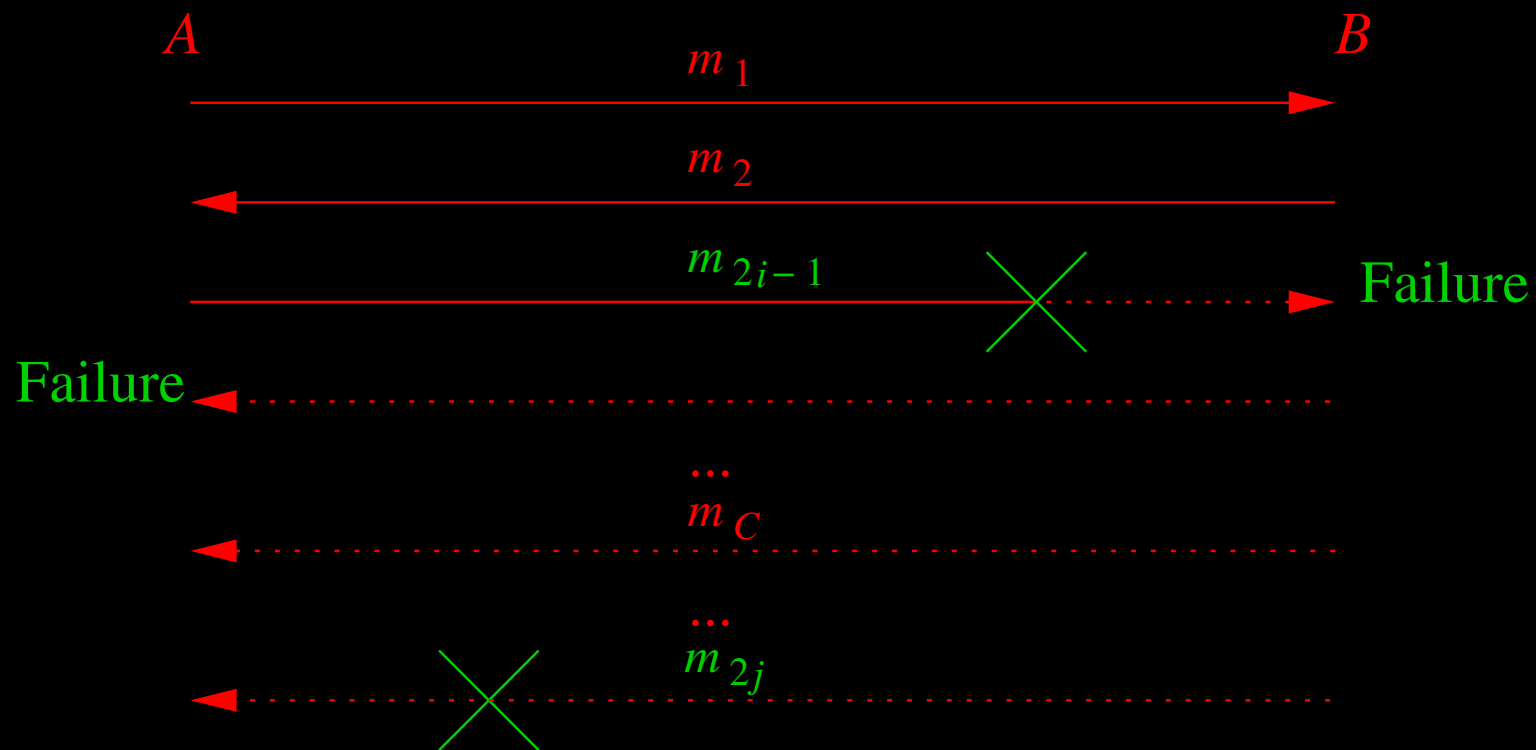
Probability of unfairness (3)

If $2i - 1 < 2j$ and $2i - 1 \leq C$, then the misbehavior of P_B has no influence since G_B is expecting the $(2i - 1)$ th message.



Probability of unfairness (4)

If $C > 2i - 1$ then the protocol “fairly” fails since G_A is also expecting a message.



Probability of unfairness (5)

Hence, if $2^i - 1 < 2^j$ then the protocol is unfair if and only if $2^i - 1 = C$, then it is unfair with probability p_{2^i-1} .

Conversely, if $2^i - 1 > 2^j$ then the protocol is unfair with probability p_{2^j} .

Therefore we have

$$P_a = \max_i p_i.$$



Probability that crime pays...

When a misbehavior drops the message i , the conditional probability that the crime pays is

$$\Pr[C = i / C \geq i].$$

Hence we have

$$P_c = \max_i \frac{p_i}{\sum_{j \geq i} p_j}.$$



e.g. 1: Uniform distribution

If $p_1 = \dots = p_n = \frac{1}{n}$ and $p_i = 0$ for $i > n$ then

$$E(C) = \frac{n+1}{2}, P_a = \frac{1}{n}, \text{ and } P_c = 1 (\text{for } i = n).$$

If the Pirate who is assumed to send the n th message does not forward it, then his risk is void since this is the last message for sure. Hence the protocol is unfair with probability $\frac{1}{n}$ but with no risk at all for Pirates.



e.g. 2: Geometric distribution

If $p_i = (1 - p)^{i-1}p$ for $i > 0$ then

$$E(C) = \frac{1}{p}, P_a = p, \text{ and } P_c = p.$$

This example is equivalent to the case where each Guardian Angel flips a coin in order to send the last message with probability p in every step.



Optimal case

We could prove (see the full paper) that the uniform distribution is the optimal case for P_a and that the geometric distribution is the optimal case for P_c .



Conclusion

We have designed a Fair Exchange protocol which

- Does not require a TTP.
- Requires no computational assumption.
- Provides arbitrarily low unfairness.

